

Citrix CloudPlatform (powered by Apache CloudStack) Version 3.0.4 Patch A Release Notes

Revised November 5, 2012 4:35 pm Pacific

**WARNING: Security Vulnerability Reported.
Immediate Action Advised. See [Security Vulnerability](#).**

Citrix CloudPlatform (powered by Apache CloudStack) Version 3.0.4 Patch A Release Notes

Revised November 5, 2012 4:35 pm Pacific: WARNING: Security Vulnerability Reported. Immediate Action Advised. See [Security Vulnerability](#).

© 2012 Citrix Systems, Inc. All rights reserved. Specifications are subject to change without notice. Citrix Systems, Inc., the Citrix logo, Citrix XenServer, Citrix XenCenter, and CloudPlatform are trademarks or registered trademarks of Citrix Systems, Inc. All other brands or products are trademarks or registered trademarks of their respective holders.

Release notes for CloudPlatform 3.0.4 Patch A.

1. Security Vulnerability Reported: Immediate Action Advised	1
2. Submitting Feedback and Getting Help	3
3. Upgrade Instructions	5
3.1. Upgrade from 3.0.x to 3.0.4 Patch A	5
3.2. Upgrade from 2.2.x to 3.0.4 Patch A	11
3.3. Upgrade from 2.1.x to 3.0.4 Patch A	20
4. Version 3.0.4 Patch A	21
4.1. What's New in 3.0.4 Patch A	21
4.2. Issues Fixed in 3.0.4 Patch A	21
5. Version 3.0.4	23
5.1. What's New in 3.0.4	23
5.2. Issues Fixed in 3.0.4	23
5.3. Known Issues in 3.0.4	23

Security Vulnerability Reported: Immediate Action Advised

We have received a report of a serious security vulnerability in CloudStack and CloudPlatform. The vulnerability allows an attacker to use a system account to issue any CloudStack API command as an administrator. The attacker could, for example, delete all VMs in the system.

We have verified that this vulnerability exists on all CloudStack and CloudPlatform versions.

At this time, we believe knowledge of the vulnerability is limited to a few individuals. No known exploits have occurred. However, we still recommend urgent action, particularly for public clouds.



Warning

This is a serious vulnerability that requires your immediate attention and action.

Action Required

The vulnerability can be fixed with a single MySQL command.

1. Log in to MySQL:

```
[root@host] # mysql -u cloud -p your-password -h host-ip-address
```

2. Add a random password to the system account:

```
MySQL> update `cloud`.`user` set password=RAND() where id=1;
```


Submitting Feedback and Getting Help

The support team is available to help customers plan and execute their installations. To contact the support team, log in to [the Support Portal](#)¹ by using the account credentials you received when you purchased your support contract.

¹ <http://support.citrix.com/cms/kc/cloud-home/>

Upgrade Instructions

3.1. Upgrade from 3.0.x to 3.0.4 Patch A

Perform the following to upgrade from version 3.0.0, 3.0.1, 3.0.2, 3.0.3, or 3.0.4 to version 3.0.4 Patch A.

1. If you are upgrading from 3.0.0 or 3.0.1, ensure that you query your IP address usage records and process them; for example, issue invoices for any usage that you have not yet billed users for.

Starting in 3.0.2, the usage record format for IP addresses is the same as the rest of the usage types. See [bug CS-8222¹](#)). Instead of a single record with the assignment and release dates, separate records are generated per aggregation period with start and end dates. After upgrading, any existing IP address usage records in the old format will no longer be available.

2. Stop all Usage Servers if running. Run this on all Usage Server hosts.

```
# service cloud-usage stop
```

3. Stop the Management Servers. Run this on all Management Server hosts.

```
# service cloud-management stop
```

4. On the MySQL master, take a backup of the MySQL databases. We recommend performing this step even in test upgrades. If there is an issue, this will assist with debugging.

In the following commands, it is assumed that you have set the root password on the database, which is a CloudPlatform recommended best practice. Substitute your own MySQL root password.

```
# mysqldump -u root -p<mysql_password> cloud >> cloud-backup.dmp
# mysqldump -u root -p<mysql_password> cloud_usage > cloud-usage-backup.dmp
```

5. Download CloudPlatform 3.0.4 Patch A onto the management server host where it will run. Get the software from the following link:

<https://www.citrix.com/English/ss/downloads/>.

You need a [My Citrix Account²](#).

6. Upgrade the CloudPlatform packages. You should have a file in the form of “CloudStack-3.0.4-N-OSVERSION.tar.gz”. Untar the file, then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-3.0.4-N-OSVERSION.tar.gz
# cd CloudStack-3.0.4-N-OSVERSION
# ./install.sh
```

You should see a few messages as the installer prepares, followed by a list of choices.

¹ <http://bugs.cloudstack.org/browse/CS-8222>

² <http://www.citrix.com/lang/English/publicindex.asp?destURL=%2FEnglish%2FmyCitrix%2Findex.asp%3F#>

7. Choose "U" to upgrade the package

```
>U
```

You should see some output as the upgrade proceeds, ending with a message like "Complete! Done."

8.  **Note**

If you are upgrading from 3.0.4, you can skip this step.

If you have made changes to your existing copy of the file `components.xml` in your previous-version CloudPlatform installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 3.0.4.



How will you know whether you need to do this? If the upgrade output in the previous step included a message like the following, then some custom content was found in your old `components.xml`, and you need to merge the two files:

```
warning: /etc/cloud/management/components.xml created as /etc/cloud/management/
components.xml.rpmnew
```

- a. Make a backup copy of your `/etc/cloud/management/components.xml` file. For example:

```
# mv /etc/cloud/management/components.xml /etc/cloud/management/components.xml-backup
```

- b. Copy `/etc/cloud/management/components.xml.rpmnew` to create a new `/etc/cloud/management/components.xml`:

```
# cp -ap /etc/cloud/management/components.xml.rpmnew /etc/cloud/management/
components.xml
```

- c. Merge your changes from the backup file into the new `components.xml` file.

```
# vi /etc/cloud/management/components.xml
```

9. Repeat steps 5 - 8 on each management server node.
10. Start the first Management Server. Do not start any other Management Server nodes yet.

```
# service cloud-management start
```

Wait until the databases are upgraded. Ensure that the database upgrade is complete. After confirmation, start the other Management Servers one at a time by running the same command on each node.

**Note**

Failing to restart the Management Server indicates a problem in the upgrade. Having the Management Server restarted without any issues indicates that the upgrade is successfully completed.

11. Start all Usage Servers (if they were running on your previous version). Perform this on each Usage Server host.

```
# service cloud-usage start
```

12. (KVM only) Additional steps are required for each KVM host. These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.

- a. Copy the CloudPlatform 3.0.4 Patch A tar file to the host, untar it, and change directory to the resulting directory.
- b. Stop the running agent.

```
# service cloud-agent stop
```

- c. Update the agent software.

```
# ./install.sh
```

- d. Choose "U" to update the packages.
- e. Start the agent.

```
# service cloud-agent start
```

13. Log in to the CloudPlatform UI as administrator, and check the status of the hosts. All hosts should come to Up state (except those that you know to be offline). You may need to wait 20 or 30 minutes, depending on the number of hosts.

**Note**

Troubleshooting: If login fails, clear your browser cache and reload the page.

Do not proceed to the next step until the hosts show in Up state. If the hosts do not come to the Up state, contact support.

14. If you are upgrading from 3.0.1 or 3.0.2, perform the following:
 - a. Ensure that the admin port is set to 8096 by using the "integration.api.port" global parameter.

This port is used by the cloud-sysvmadm script at the end of the upgrade procedure. For information about how to set this parameter, see “Edit the Global Configuration Settings” in the Advanced Installation Guide.

- b. Restart the Management Server.



Note

If you don't want the admin port to remain open, you can set it to null after the upgrade is done and restart the management server

15. Run the following script to stop, then start, all Secondary Storage VMs, Console Proxy VMs, and virtual routers. Run the script once on one management server. The script requires the IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-a" argument. For example:

```
# nohup cloud-sysvmadm -d 192.168.1.5 -u cloud -p password -a > sysvm.log 2>&1 &
# tail -f sysvm.log
```

This might take up to an hour or more to run, depending on the number of accounts in the system.

16. In order to deploy AWS API on its new port (7080), you need to deploy it under a separate webapps folder and make some changes to port settings.

- a. Create the new webapps folder:

```
# mkdir -p /usr/share/cloud/management/webapps7080
```

- b. Create a symbolic link:

```
# ln -s /usr/share/cloud/bridge/webapps/awsapi /usr/share/cloud/management/
webapps7080/awsapi
```

- c. Remove the old folder:

```
# rm /usr/share/cloud/management/webapps/awsapi
```

- d. Open port 7080:

```
# iptables -I INPUT -p tcp -m tcp --dport 7080 -j ACCEPT
```

- e. If you have made any modifications in server.xml on your existing CloudPlatform installation, back it up:

```
# mv /etc/cloud/management/server.xml /etc/cloud/management/server.xml-backup
```

Then replace with the new server.xml file:

```
# cp /etc/cloud/management/server.xml.rpmnew /etc/cloud/management/server.xml
```

Merge any changes from the backup file into the new server.xml file.

```
# vi /etc/cloud/management/server.xml
```

- f. Open the `/etc/cloud/management/ec2.service.properties` file in your favorite editor. For example:

```
# vi /etc/cloud/management/ec2.service.properties
```

Add the following to specify the Management Server host and port to which AWS API calls should be forwarded. Substitute your actual Management Server IP address.

```
managementServer=<management.server.IP.address>  
cloudAPIPort=8080
```

- g. Restart the Management Server to put the new settings into effect.
17. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudPlatform 3.0.4. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudPlatform 3.0.3 Advanced Installation Guide.
18. Now apply the XenServer hotfix XS602E003 to XenServer v6.0.2 hypervisor hosts. (Support for this hotfix is the reason for release 3.0.4.)
- a. Disconnect the XenServer cluster from CloudPlatform.

In the left navigation bar of the CloudPlatform UI, select Infrastructure. Under Clusters, click View All. Select the XenServer cluster and click Actions - Unmanage.

This may fail if there are hosts not in one of the states Up, Down, Disconnected, or Alert. You may need to fix that before unmanaging this cluster.

Wait until the status of the cluster has reached Unmanaged. Use the CloudPlatform UI to check on the status. When the cluster is in the unmanaged state, there is no connection to the hosts in the cluster.

- b. To clean up the VLAN, log in to one XenServer host and run:

```
/opt/xensource/bin/cloud-clean-vlan.sh
```

- c. Now prepare the upgrade by running the following on one XenServer host:

```
/opt/xensource/bin/cloud-prepare-upgrade.sh
```


If you see a message like "can't eject CD", log in to the VM and umount the CD, then run this script again.

- d. Upload the hotfix to the XenServer hosts. Always start with the Xen pool master, then the slaves. Using your favorite file copy utility (e.g. WinSCP), copy the hotfixes to the host. Place them in a temporary folder such as `/root` or `/tmp`.

On the Xen pool master, upload the hotfix with this command:

```
xe patch-upload file-name=XS602E003.xsupdate
```

Make a note of the output from this command, which is a UUID for the hotfix file. You'll need it in another step later.

 **Note**

(Optional) If you are applying other hotfixes as well, you can repeat the commands in this section with the appropriate hotfix number. For example, XS602E004.xsupdate.

- e. Manually live migrate all VMs on this host to another host. First, get a list of the VMs on this host:

```
# xe vm-list
```

Then use this command to migrate each VM. Replace the example host name and VM name with your own:

```
# xe vm-migrate live=true host=<host-name> vm=<VM-name>
```

Troubleshooting: If you see a message like "You attempted an operation on a VM which requires PV drivers to be installed but the drivers were not detected," run `/opt/xensource/bin/make_migratable.sh b6cf79c8-02ee-050b-922f-49583d9f1a14`.

- f. Apply the hotfix. First, get the UUID of this host:

```
# xe host-list
```

Then use the following command to apply the hotfix. Replace the example host UUID with the current host ID, and replace the hotfix UUID with the output from the patch-upload command you ran on this machine earlier. You can also get the hotfix UUID by running `xe patch-list`.

```
xe patch-apply host-uuid=<host-uuid> uuid=<hotfix-uuid>
```

- g. Copy the following files from the CloudPlatform Management Server to the host.

Copy from here...	...to here
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/xenserver60/NFSSR.py	/opt/xensource/sm/NFSSR.py
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/setupxenserver.sh	/opt/xensource/bin/setupxenserver.sh
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/make_migratable.sh	/opt/xensource/bin/make_migratable.sh

- h. Reboot this XenServer host.
- i. Run the following:

```
/opt/xensource/bin/setupxenserver.sh
```



Note

If the message "mv: cannot stat `/etc/cron.daily/logrotate`: No such file or directory" appears, you can safely ignore it.

- j. Run the following:

```
for pbd in `xe pbd-list currently-attached=false | grep ^uuid | awk '{print $NF}'`; do
  xe pbd-plug uuid=$pbd ;
```

- k. On each slave host in the Xen pool, repeat these steps, starting from "manually live migrate VMs."

3.2. Upgrade from 2.2.x to 3.0.4 Patch A

1. Ensure that you query your IPaddress usage records and process them; for example, issue invoices for any usage that you have not yet billed users for.

Starting in 3.0.2, the usage record format for IP addresses is the same as the rest of the usage types. See [CS-8222](#)³. Instead of a single record with the assignment and release dates, separate records are generated per aggregation period with start and end dates. After upgrading to 3.0.4, any existing IP address usage records in the old format will no longer be available.

2. If you are using version 2.2.0 - 2.2.13, first upgrade to 2.2.14 by using the instructions in the 2.2.14 Release Notes.



Note

(KVM only) If KVM hypervisor is used in your cloud, be sure you completed the step to insert a valid username and password into the host_details table on each KVM node as described in the 2.2.14 Release Notes. This step is critical, as the database will be encrypted after the upgrade to 3.0.4.

3. While running the 2.2.14 system, log in to the UI as root administrator.
4. Using the UI, add a new System VM template for each hypervisor type that is used in your cloud. In each zone, add a system VM template for each hypervisor used in that zone
 - a. In the left navigation bar, click Templates.

³ <http://bugs.cloudstack.org/browse/CS-8222>

- b. In Select view, click Templates.
- c. Click Register template.

The Register template dialog box is displayed.

- d. In the Register template dialog box, specify the following values depending on the hypervisor type (do not change these):

Hypervisor	Description
XenServer	<p>Name: systemvm-xenserver-3.0.0</p> <p>Description: systemvm-xenserver-3.0.0</p> <p>URL: http://download.cloud.com/templates/acton/acton-systemvm-02062012.vhd.bz2</p> <p>Zone: Choose the zone where this hypervisor is used</p> <p>Hypervisor: XenServer</p> <p>Format: VHD</p> <p>OS Type: Debian GNU/Linux 5.0 (32-bit)</p> <p>Extractable: no</p> <p>Password Enabled: no</p> <p>Public: no</p> <p>Featured: no</p>
KVM	<p>Name: systemvm-kvm-3.0.0</p> <p>Description: systemvm-kvm-3.0.0</p> <p>URL: http://download.cloud.com/templates/acton/acton-systemvm-02062012.qcow2.bz2</p> <p>Zone: Choose the zone where this hypervisor is used</p> <p>Hypervisor: KVM</p> <p>Format: QCOW2</p> <p>OS Type: Debian GNU/Linux 5.0 (32-bit)</p> <p>Extractable: no</p> <p>Password Enabled: no</p> <p>Public: no</p> <p>Featured: no</p>
VMware	<p>Name: systemvm-vmware-3.0.0</p> <p>Description: systemvm-vmware-3.0.0</p>

Hypervisor	Description
	URL: http://download.cloud.com/templates/acton/acton-systemvm-02062012.ova Zone: Choose the zone where this hypervisor is used Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 5.0 (32-bit) Extractable: no Password Enabled: no Public: no Featured: no

5. Watch the screen to be sure that the template downloads successfully and enters the READY state. Do not proceed until this is successful
6. **WARNING:** If you use more than one type of hypervisor in your cloud, be sure you have repeated these steps to download the system VM template for each hypervisor type. Otherwise, the upgrade will fail.
7. Stop all Usage Servers if running. Run this on all Usage Server hosts.

```
# service cloud-usage stop
```

8. Stop the Management Servers. Run this on all Management Server hosts.

```
# service cloud-management stop
```

9. On the MySQL master, take a backup of the MySQL databases. We recommend performing this step even in test upgrades. If there is an issue, this will assist with debugging.

In the following commands, it is assumed that you have set the root password on the database, which is a CloudPlatform recommended best practice. Substitute your own MySQL root password.

```
# mysqldump -u root -p<mysql_password> cloud >> cloud-backup.dmp
# mysqldump -u root -p<mysql_password> cloud_usage > cloud-usage-backup.dmp
```

10. Download CloudPlatform 3.0.4 Patch A onto the management server host where it will run. Get the software from the following link:

<https://www.citrix.com/English/ss/downloads/>

You need a [My Citrix Account](#)⁴.

⁴ <http://www.citrix.com/lang/English/publicindex.asp?destURL=%2FEnglish%2FmyCitrix%2Findex.asp%3F#>

11. Upgrade the CloudPlatform packages. You should have a file in the form of "CloudStack-3.0.4-N-OSVERSION.tar.gz". Untar the file, then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-3.0.4-N-OSVERSION.tar.gz
# cd CloudStack-3.0.4-N-OSVERSION
# ./install.sh
```

You should see a few messages as the installer prepares, followed by a list of choices.

12. Choose "U" to upgrade the package

```
>U
```

You should see some output as the upgrade proceeds, ending with a message like "Complete! Done."

13. If you have made changes to your existing copy of the file components.xml in your previous-version CloudPlatform installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 3.0.4.



Note

How will you know whether you need to do this? If the upgrade output in the previous step included a message like the following, then some custom content was found in your old components.xml, and you need to merge the two files:

```
warning: /etc/cloud/management/components.xml created as /etc/cloud/management/
components.xml.rpmnew
```

- a. Make a backup copy of your /etc/cloud/management/components.xml file. For example:

```
# mv /etc/cloud/management/components.xml /etc/cloud/management/components.xml-backup
```

- b. Copy /etc/cloud/management/components.xml.rpmnew to create a new /etc/cloud/management/components.xml:

```
# cp -ap /etc/cloud/management/components.xml.rpmnew /etc/cloud/management/
components.xml
```

- c. Merge your changes from the backup file into the new components.xml file.

```
# vi /etc/cloud/management/components.xml
```

14. If you have made changes to your existing copy of the /etc/cloud/management/db.properties file in your previous-version CloudPlatform installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 3.0.4.

- a. Make a backup copy of your file /etc/cloud/management/db.properties. For example:

```
# mv /etc/cloud/management/db.properties /etc/cloud/management/db.properties-backup
```

- b. Copy `/etc/cloud/management/db.properties.rpmnew` to create a new `/etc/cloud/management/db.properties`:

```
# cp -ap /etc/cloud/management/db.properties.rpmnew /etc/cloud/management/db.properties
```

- c. Merge your changes from the backup file into the new `db.properties` file.

```
# vi /etc/cloud/management/db.properties
```

15. On the management server node, run the following command. It is recommended that you use the command-line flags to provide your own encryption keys. See [Password and Key Encryption in the Installation Guide](#).

```
# cloud-setup-encryption -e <encryption_type> -m <management_server_key> -k <database_key>
```

When used without arguments, as in the following example, the default encryption type and keys will be used:

- (Optional) For `encryption_type`, use `file` or `web` to indicate the technique used to pass in the database encryption password. Default: `file`.
- (Optional) For `management_server_key`, substitute the default key that is used to encrypt confidential parameters in the properties file. Default: `password`. It is highly recommended that you replace this with a more secure value
- (Optional) For `database_key`, substitute the default key that is used to encrypt confidential parameters in the CloudPlatform database. Default: `password`. It is highly recommended that you replace this with a more secure value.

16. Repeat steps 10 - 15 on every management server node. If you provided your own encryption key in step 15, use the same key on all other management servers.
17. Start the first Management Server. Do not start any other Management Server nodes yet.

```
# service cloud-management start
```

Wait until the databases are upgraded. Ensure that the database upgrade is complete. You should see a message like "Complete! Done." After confirmation, start the other Management Servers one at a time by running the same command on each node.

18. Start all Usage Servers (if they were running on your previous version). Perform this on each Usage Server host.

```
# service cloud-usage start
```

19. (KVM only) Additional steps are required for each KVM host. These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.

Chapter 3. Upgrade Instructions

- a. Copy the CloudStack 3.0.4 Patch A .tgz download to the host, untar it, and cd into the resulting directory.
- b. Stop the running agent.

```
# service cloud-agent stop
```

- c. Update the agent software.

```
# ./install.sh
```

- d. Choose "U" to update the packages.
- e. Start the agent.

```
# service cloud-agent start
```

20. Log in to the CloudPlatform UI as admin, and check the status of the hosts. All hosts should come to Up state (except those that you know to be offline). You may need to wait 20 or 30 minutes, depending on the number of hosts.

Do not proceed to the next step until the hosts show in the Up state. If the hosts do not come to the Up state, contact support.

21. Run the following script to stop, then start, all Secondary Storage VMs, Console Proxy VMs, and virtual routers.
 - a. Run the command once on one management server. Provide the IP address of the MySQL instance, the MySQL user name, and the database password for that user. In addition to those parameters, provide the "-a" argument. For example:

```
# nohup cloud-sysvmadm -d 192.168.1.5 -u cloud -p password -a > sysvm.log 2>&1 &
```

This might take up to an hour or more to run, depending on the number of accounts in the system.

- b. After the script terminates, check the log to verify correct execution:

```
# tail -f sysvm.log
```

The content should be like the following:

```
Stopping and starting 1 secondary storage vm(s)...
Done stopping and starting secondary storage vm(s)
Stopping and starting 1 console proxy vm(s)...
Done stopping and starting console proxy vm(s).
Stopping and starting 4 running routing vm(s)...
Done restarting router(s).
```

22. If you would like additional confirmation that the new system VM templates were correctly applied when these system VMs were rebooted, SSH into the System VM and check the version.

Use one of the following techniques, depending on the hypervisor.

XenServer or KVM:

SSH in by using the link local IP address of the system VM. For example, in the command below, substitute your own path to the private key used to log in to the system VM and your own link local IP.

Run the following commands on the XenServer or KVM host on which the system VM is present:

```
# ssh -i <private-key-path> <link-local-ip> -p 3922
# cat /etc/cloudstack-release
```

The output should be like the following:

```
Cloudstack Release 3.0 Mon Feb 6 15:10:04 PST 2012
```

ESXi

SSH in using the private IP address of the system VM. For example, in the command below, substitute your own path to the private key used to log in to the system VM and your own private IP.

Run the following commands on the Management Server:

```
# ssh -i <private-key-path> <private-ip> -p 3922
# cat /etc/cloudstack-release
```

The output should be like the following:

```
Cloudstack Release 3.0 Mon Feb 6 15:10:04 PST 2012
```

23. In order to deploy AWS API on its new port (7080), you need to deploy it under a separate webapps folder.

a. Create the new webapps folder:

```
# mkdir -p /usr/share/cloud/management/webapps7080
```

b. Create a symbolic link:

```
# ln -s /usr/share/cloud/bridge/webapps/awsapi /usr/share/cloud/management/
webapps7080/awsapi
```

c. Remove the old folder:

```
# rm /usr/share/cloud/management/webapps/awsapi
```

d. Open port 7080:

```
# iptables -I INPUT -p tcp -m tcp --dport 7080 -j ACCEPT
```

- e. If you have made any modifications in `server.xml` on your existing CloudPlatform installation, back it up:

```
# mv /etc/cloud/management/server.xml /etc/cloud/management/server.xml-backup
```

Then replace with the new `server.xml` file:

```
# cp /etc/cloud/management/server.xml.rpmnew /etc/cloud/management/server.xml
```

Merge any changes from the backup file into the new `server.xml` file.

```
# vi /etc/cloud/management/server.xml
```

- f. Open the `/etc/cloud/management/ec2.service.properties` file in your favorite editor. For example:

```
# vi /etc/cloud/management/ec2.service.properties
```

Add the following to specify the Management Server host and port to which AWS API calls should be forwarded.

```
managementServer=<management.server.IP.address>  
cloudAPIPort=8080
```

- g. Restart the Management Server to put the new settings into effect.
24. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudPlatform 3.0.4. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudPlatform 3.0.3 Advanced Installation Guide.
 25. Now apply the XenServer hotfix XS602E003 to XenServer v6.0.2 hypervisor hosts. (Support for this hotfix is the reason for release 3.0.4.)

- a. Disconnect the XenServer cluster from CloudPlatform.

In the left navigation bar of the CloudPlatform UI, select Infrastructure. Under Clusters, click View All. Select the XenServer cluster and click Actions - Unmanage.

This may fail if there are hosts not in one of the states Up, Down, Disconnected, or Alert. You may need to fix that before unmanaging this cluster.

Wait until the status of the cluster has reached Unmanaged. Use the CloudPlatform UI to check on the status. When the cluster is in the unmanaged state, there is no connection to the hosts in the cluster.

- b. To clean up the VLAN, log in to one XenServer host and run:

```
/opt/xensource/bin/cloud-clean-vlan.sh
```

- c. Now prepare the upgrade by running the following on one XenServer host:

```
/opt/xensource/bin/cloud-prepare-upgrade.sh
```

If you see a message like "can't eject CD", log in to the VM and umount the CD, then run this script again.

- d. Upload the hotfix to the XenServer hosts. Always start with the Xen pool master, then the slaves. Using your favorite file copy utility (e.g. WinSCP), copy the hotfixes to the host. Place them in a temporary folder such as /root or /tmp.

On the Xen pool master, upload the hotfix with this command:

```
xe patch-upload file-name=XS602E003.xsupdate
```

Make a note of the output from this command, which is a UUID for the hotfix file. You'll need it in another step later.



Note

(Optional) If you are applying other hotfixes as well, you can repeat the commands in this section with the appropriate hotfix number. For example, XS602E004.xsupdate.

- e. Manually live migrate all VMs on this host to another host. First, get a list of the VMs on this host:

```
# xe vm-list
```

Then use this command to migrate each VM. Replace the example host name and VM name with your own:

```
# xe vm-migrate live=true host=<host-name> vm=<VM-name>
```

Troubleshooting: If you see a message like "You attempted an operation on a VM which requires PV drivers to be installed but the drivers were not detected," run `/opt/xensource/bin/make_migratable.sh b6cf79c8-02ee-050b-922f-49583d9f1a14`.

- f. Apply the hotfix. First, get the UUID of this host:

```
# xe host-list
```

Then use the following command to apply the hotfix. Replace the example host UUID with the current host ID, and replace the hotfix UUID with the output from the patch-upload command you ran on this machine earlier. You can also get the hotfix UUID by running `xe patch-list`.

```
xe patch-apply host-uuid=<host-uuid> uuid=<hotfix-uuid>
```

- g. Copy the following files from the CloudPlatform Management Server to the host.

Copy from here...	...to here
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/xenserver60/NFSSR.py	/opt/xensource/sm/NFSSR.py
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/setupxenserver.sh	/opt/xensource/bin/setupxenserver.sh
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/make_migratable.sh	/opt/xensource/bin/make_migratable.sh

- h. Reboot this XenServer host.
- i. Run the following:

```
/opt/xensource/bin/setupxenserver.sh
```



Note

If the message "mv: cannot stat `/etc/cron.daily/logrotate': No such file or directory" appears, you can safely ignore it.

- j. Run the following:

```
for pbd in `xe pbd-list currently-attached=false | grep ^uuid | awk '{print $NF}'`; do  
xe pbd-plug uuid=$pbd ;
```

- k. On each slave host in the Xen pool, repeat these steps, starting from "manually live migrate VMs."

3.3. Upgrade from 2.1.x to 3.0.4 Patch A

Direct upgrades from version 2.1.0 - 2.1.10 to 3.0.4 Patch A are not supported. It must first be upgraded to version 2.2.14. For information on how to upgrade from 2.1.x to 2.2.14, see the version 2.2.14 Release Notes.

Version 3.0.4 Patch A

4.1. What's New in 3.0.4 Patch A

CloudPlatform 3.0.4 Patch A is a bug fix release. There are no new features in this software package.

4.2. Issues Fixed in 3.0.4 Patch A

Defect	Description
15061	Port forwarding policies with port ranges can be defined.
15089	Optimized list* API calls to improve performance and increase accuracy of Infrastructure page in UI.
15067, 15038	Log file is no longer filled by multiple SSVMs attempting to run.
15051	Removed bottlenecks which were causing slow performance when creating new port forwarding rules.
15048	Reduced CPU usage of Management Server through optimizations.
15047	Display of system capacity statistics on Dashboard in UI has improved performance through optimization of the listCapacity API call.
15042	After stopping and starting XAPI, hosts are now properly reconnected to CloudPlatform and not stuck in the down/alert state.
15034	Load balancer rules that use port 8080 can be defined. These will no longer conflict with the password server.
15000	Users can get only the list of their own resources, not those belonging to another user within the domain.
14986	Password reset on existing VMs now works properly after upgrading. Resolved conflicting techniques for setting the IP address of the password server in old script vs. new script.
15094	Additional interfaces (such as eth3, eth4) now come up properly after stopping the master router in a guest network with multiple redundant virtual routers (RVRs).
CS-16432	listVolumes API returns all fields.
CS-16431	Volumes screen in UI now has attach disk and detach disk icons.
CS-16426	In a network where conserve mode is off, you can create PF, LB, and firewall rules even if the firewall rule is created first.
CS-16405	Infrastructure page in UI now shows correct number of routers.
CS-16404	"View Users" button in the UI now shows user details.
CS-16403	Can restart the cloud service on SSVM.
CS-13836	Outbound access is possible from a VM that is deployed with two networks, isolated network with source NAT and shared network.

Version 3.0.4

5.1. What's New in 3.0.4

CloudPlatform 3.0.4 is the first maintenance patch for CloudPlatform 3.0.3. This release includes no new features. For a list of the major fixed items, see Issues Fixed in 3.0.4.

5.2. Issues Fixed in 3.0.4

Defect	Description
CS-15376, CS-15373	The AWS APIs (EC2 and S3) now listen on the 7080 port and send request to CloudStack on the 8080 port just as any other clients of CloudStack.
CS-13944	The CloudPlatform 2.2.x to 3.0.x database upgrade for multiple physical networks is now supported.
CS-15300	The admin accounts of a domain now honour the limits imposed on that domain just like the regular accounts do. A domain admin now is not allowed to create an unlimited number of instances, volumes, snapshots, and so on.
CS-15396	The CloudPlatform database now contain the UUD information after the 2.2.14 to 3.0.4 upgrade.
CS-15450	Upgrade from 2.2.14 to 3.0.4 no longer fails on a VMware host.
CS-15449	Running cloudstack-aws-api-register no longer fails with the "User registration failed with error: [Errno 113] No route to host" error.
CS-15455	The iptable rules are configured to open the awsapi port (7080) as part of the installation.
CS-15429	While creating an instance with data volume, disk offering also is considered while checking the account limit on volume resources.
CS-15414	After the 2.2.14 to 3.0.4 upgrade, the value of the global parameter xen.guest.network.device is now decrypted before setting the traffic label.
CS-15382	During 2.2.14 to 3.0.4 upgrade, the hosts no longer go to the Alert state if destroyed networks existed with non-existent tags prior to upgrade.
CS-15323	CloudPlatform supports the following Citrix XenServer hotfixes: XS602E003, XS602E004, and XS602E005.
CS-15430	Create snapshot now fails if creating a snapshot exceeds the snapshot resource limit for a domain admin or a user account.


5.3. Known Issues in 3.0.4

Issue ID	Description
CS-11514 (was 11535)	In-line mode for load balancer is not supported for all external devices.
CS-12624 (was 12741)	vSphere: maintenance mode will not live migrate system VM to another host.

Issue ID	Description
CS-12714 (was 12840)	Capacity view is not available for pods or clusters.
CS-13173 (was 13336)	vSphere: cross cluster volume migration does not work properly.
CS-13192 (was 13359)	Programming F5/NetScaler rules can be better optimized.
CS-13337 (was 13518)	Security Groups are not supported in Advanced Networking
CS-13682 (was 13883)	Multiple NetScalers are not supported in Basic Networking.
CS-13733 (was 13935)	vSphere: detaching an ISO from a restored VM instance fails.
CS-13758 (was 13963)	vSphere: template download from templates created off of the root volume does not work properly.
CS-14201 (was 14430)	VMWare: Template sizes are being reported different depending on whether the primary storage is using iSCSI or NFS.
CS-14275 (was 14506)	F5: Unable to properly remove a F5 device.
CS-14291 (was 14523)	The EIP/ELB network offering for basic zones does not support multiple NetScalers.
CS-14296 (was 14530)	OVM: Network traffic labels are not supported.
CS-14303 (was 14537)	The IP addresses for a shared network are still being consumed even if no services are defined for that network.
CS-14346	The UpdateVirtualMachine API call does not check whether the VM is stopped. Therefore, stop the VM manually before issuing this call.
CS-14361	On KVM hosts, the volume size allocated in primary storage is stored incorrectly in the database or displayed incorrectly in the Dashboard. The value displayed in the Dashboard is very small compared to the original size.
CS-14452	Data disk volumes are not automatically copied from one cluster to another.
CS-14655	<p>XenServer known issue: If using network bonding on XenServer 6.0.x along with the CloudStack XenServer Support Package (CSP), interfaces, IPs, and networking can fail after adding hosts to the cloud and rebooting them. Workaround: patch each XenServer node, using the following steps. This patch is required only if using the CSP, and is a temporary requirement until XenServer issues the official hotfix for this issue. Before installing the CSP package, install the newer biosdevname rpm, selecting the correct patch for your version of XenServer: XenServer patch XS759 for XenServer 6.0.2 or XenServer patch XS753 for XenServer 6.0.0.</p> <ol style="list-style-type: none"> Download three files: <ul style="list-style-type: none"> http://download.cloud.com/releases/3.0.2/60-net.rules.template http://download.cloud.com/releases/3.0.2/net-rename-sideways.sh http://download.cloud.com/releases/3.0.2/biosdevname-0.3.7-1.xs753.i386.rpm (for XenServer

Issue ID	Description
	<p>6.0.0) or http://download.cloud.com/releases/3.0.2/biosdevname-0.3.7-1.xs759.i386.rpm (for XenServer 6.0.2)</p> <ol style="list-style-type: none"> Run the following. Substitute the filename of the patch you are using: <pre data-bbox="699 439 1441 499">rpm -ivh <packageName>.rpm -force</pre> Replace <code>/etc/udev/scripts/net-rename-sideways.sh</code> with the new version. Replace <code>/etc/sysconfig/network-scripts/interface-rename-data/60-net.rules.template</code> with the newer version. Delete <code>/etc/udev/rules.d/60-net.rules</code>.
CS-14680	<p>CloudStack and LDAP user validation cannot happen simultaneously because the user password is hashed and stored in the database, and LDAP requires the passwords in plain text.</p> <p>To work with the LDAP user, the MD5 hash should be disabled in the login process by commenting the following variable in <code>sharedFunctions.js</code> file available at <code>/usr/share/cloud/management/webapps/client/scripts</code>, and restart the cloud-management service.</p> <pre data-bbox="647 1061 1441 1122">var md5HashedLogin = false;</pre> <p>However, if <code>md5HashedLogin</code> is set to <code>false</code>, the end user can login with the LDAP credentials but not with the CloudPlatform user credentials.</p>
CS-14756	<p>Installing KVM on RHEL 6.2 will result in unreliable network performance. Workaround: blacklist <code>vhost-net</code>. Edit <code>/etc/modprobe.d/blacklist-kvm.conf</code> and include <code>vhost-net</code>.</p>
CS-14770	<p>The API does not return the keypair information when a VM is deployed with <code>sshkey</code>. This affects the API commands related to virtual machines (<code>deployVirtualMachine</code>, <code>listVirtualMachines</code>, ... <code>*VirtualMachine</code>), as well as the corresponding AWS APIs.</p>
CS-14780	<p>You are allowed to ping the elastic IP address of the VM even though no ingress rule is set that allows the ICMP protocol.</p>
CS-14796	<p>Deploying a VM is allowed even if the user data is not Base 64 encoded. Using the <code>ec2-run-instances</code> API with <code>-d</code> or <code>-f</code> option with user data in plain does not return any error.</p>
CS-14879	<p>When a user VM is stopped or terminated, the static NAT associated with this VM is not disabled. This public IP address is still owned by this account and cannot be associated to any other user VM.</p>
CS-14939	<p>Adding a VMware cluster is not supported when the Management Network is migrated to the Distributed Virtual Switch environment.</p>

Issue ID	Description
CS-14952	The vCenter IP Address and the datacenter information is not present in the "virtual_supervisor_module" table. The Nexus virtual switch credentials are not encrypted.
CS-15009	The port_profile table will not be populated with port profile information. In this release, CloudPlatform directly connects to the VSM for all the port profile operations; therefore, no port profile information is cached.
CS-15037	Hairpin NAT is not supported when NetScaler is used for EIP.
CS-15092	Connecting to the guest VMs through SSH is extremely slow, and it results in connection timeout.
CS-15105	The cloud-sysvmadm script does not work if the integration.api.port parameter is set to any port other than 8096.
CS-15117	In a deployment with Nexus 1000v virtual switch, disable/enable operation of the Nexus virtual switch is not working as expected. The Nexus 1000v virtual switch continues to be used to create network or edit network operations even after disabling the switch.
CS-15118	In a deployment with Nexus 1000v virtual switch, zone VLAN range is not validated against the reserved list of VLANs for Nexus 1000v.
CS-15120	No actions are listed in the Action column of the Volumes page in the CloudPlatform UI.
CS-15124	Mixed switch environment is not supported. The zone can either be deployed as Standard vSwitch based or Nexus virtual switch based.
CS-15163	The minimum limit is not honored when there is not enough capacity to deploy all the VMs and the ec2-run-instances command with the -n >n1 -n2> option is used to deploy multiple VMs.
CS-15167	The Amazon Web Services API does not allow the admin user to view or act on the resources owned by the regular users.
CS-15198	Peak bandwidth (PIR) and burst size shaping policies are not applied on Nexus 1000v virtual switch interface.
CS-15218	You might find the term "CloudStack" when you expect "CloudPlatform" in scripts, file names, etc. The use of the new product name CloudPlatform is not yet fully implemented.
CS-15256	<p>If cluster addition fails in a zone using the Cisco Nexus 1000v virtual switch, a subsequent retry will not succeed in adding the cluster. To work around:</p> <ol style="list-style-type: none"> 1. Find the VSM id that was attempted to be added along with the cluster when the cluster creation failed. To do this, log into the MySQL database and execute a select query: <pre data-bbox="608 1883 1342 2047"> # mysql -uroot -p <password_for_mysql_db>; mysql> use cloud; mysql> select id from `cloud`.`virtual_supervisor_module` where ipaddr="<vsm_ipaddress>"; </pre>

Issue ID	Description
	<p>2. Delete the cluster to VSM mapping in the cluster_vsm_map table for this vsm id:</p> <pre data-bbox="699 342 1441 432" style="border: 1px solid gray; padding: 5px;">mysql> delete from `cloud`.`virtual_supervisor_module` where vsm_id=<the id returned in step1>;</pre> <p>3. Try again to add the cluster.</p>
CS-15407	<p>After the 2.2.14 to 3.0.4 upgrade, VLAN allocation on multiple physical networks does not happen as expected.</p> <p>To workaround this issue, follow the instructions given below:</p> <ol style="list-style-type: none"> 1. Revert to your 2.2.14 setup. 2. Stop all the VMs with the isolated virtual networks in your cloud setup. 3. Run following query to find if any networks still have the NICs allocated: <ol style="list-style-type: none"> a. Check if any virtual guest networks have the NICs allocated: <pre data-bbox="746 1014 1441 1126" style="border: 1px solid gray; padding: 5px;">#SELECT DISTINCT op.id from `cloud`.`op_networks` op JOIN `cloud`.`networks` n on op.id=n.id WHERE nics_count != 0 AND guest_type = 'Virtual';</pre> b. If this returns any network IDs, then ensure the following: <ol style="list-style-type: none"> i. All the VMs are stopped. ii. No new VM is started. iii. Shutdown the Management Server. c. Remove the NICs count for the virtual network IDs returned in step (a), and set the NIC count to 0: <pre data-bbox="746 1507 1441 1585" style="border: 1px solid gray; padding: 5px;">UPDATE `cloud`.`op_networks` SET nics_count = 0 WHERE id = <enter id of virtual network></pre> d. Restart the Management Server, and wait for all the networks to shut down. <div data-bbox="746 1686 1441 1899" style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Note</p> <p>Networks shutdown is determined by the network.gc.interval and network.gc.wait parameters.</p> </div> 4. Ensure that all the networks are shut down and all the guest VNETs are free.

Issue ID	Description
	<p>5. Run the upgrade script.</p> <p>This allocates all your guest VNET ranges to the first physical network.</p> <p>6. By using the updatePhysicalNetwork API, reconfigure the VNET ranges for each physical network as desired.</p> <p>7. Start all the VMs.</p>
CS-15476	The 2.2.14 to 3.0.4 upgrade fails if multiple untagged physical networks exist before the upgrade.
CS-15578	<p>Upgrade from 2.2.14 to 3.04 fails with an exception if the setup has a zone deleted and the corresponding router state removed.</p> <p>To workaround this issue, perform the following before upgrading from 2.2.x to 3.0.4:</p> <pre data-bbox="560 819 1350 936"># mysql> delete dr from domain_router dr, vm_instance vi, data_center dc where dr.id = vi.id and vi.data_center_id = dc.id and dc.removed is not null;</pre>
CS-16601, CS-15316	Japanese keyboard is not supported.
Many	Bare metal host provisioning is not working properly.